UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
GREENBELT DIVISION

BONNIE TAYLOR,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC.
10400 Fernwood Road
Bethesda, MD 20817,

and

STARWOOD HOTELS & RESORTS WORLDWIDE, LLC
One Star Point
Stamford, CT 06902,

Defendants.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Bonnie Taylor ("Plaintiff") on behalf of herself and all others similarly situated, brings this class action against Marriott International, Inc. ("Marriott International") and Starwood Hotels and Resorts Worldwide, LLC ("Starwood") (collectively, "Marriott" or "Defendants"), based on personal knowledge as to herself and on information and belief based on the investigation of counsel, and public sources as to other matters:

NATURE OF THE ACTION

1. On November 30, 2018, Marriott International—the world's largest lodging company—announced the second largest data breach in history (the "Starwood Breach"). An unauthorized party had copied data for 500 million guests, including guests' names, birthdates, passport numbers, mailing addresses, phone numbers, encrypted payment card numbers and expiration dates ("Payment Data"), and other personal information from Starwood's guest database (the "Starwood Database").[1] Worse still, hackers appear to have had access to the Starwood Database for at least four years, going back to 2014, and the hackers may have gained access to the keys to decrypt Payment Data during that time.

2. That the cybercriminals have both copied and exported guests' Personal Information[2] over the past four years is a near certainty. Once hackers gain access to a poorly

[1] The Starwood system consisted of multiple databases and sub-systems, including a Starwood Preferred Guest ("SPG") member database, the actual reservation system where active bookings are kept, and a so-called data warehouse used for analytical and marketing purposes. Plaintiff believes that the data warehouse was the subject of the Starwood Breach, but the term "Starwood Database," as used in this Complaint, should be construed expansively to cover all Starwood databases and sub-systems storing customer data. Israel del Rio-Quilmach, *I Was a Senior VP of Technology at Starwood—Here's My Take on the Guest Data Breach*, PHOCUSWIRE (Dec. 10, 2018), https://www.phocuswire.com/Marriott-data-breach-ex-Starwood-perspective.

[2] As used throughout this Complaint, "Personal Information" means all information exposed by the Starwood Breach, including all or any part or combination of name, postal address, phone number, date of birth, gender, email address, passport number, encrypted credit card data,

secured database, such as the Starwood Database, they typically leverage the target's own server resources to collect, encrypt, and export the data. While Marriott announced the detection of one large encrypted file, the fact that hackers have had unfettered access to the Starwood Database for four years suggests that there will be further revelations about the scope of the Starwood Breach.

3. Hospitality companies, particularly those with an international footprint, are widely recognized as attractive targets for cybercriminals and espionage campaigns due to the range of Personal Information in guest reservation databases and systems.

4. Marriott International acquired Starwood Hotels & Resorts Worldwide in September 2016 in a $13.6 billion transaction, creating the world's largest lodging company. But even before Marriott International completed its acquisition of Starwood, it had cause to be aware that Starwood's systems were vulnerable to attack. In November 2015—just two weeks after the Marriott-Starwood merger was announced—Starwood publicly disclosed that its point of sale ("POS") infrastructure had been infected with malware for eight months. It is unknown when Marriott International first learned of the POS infection or the Starwood Breach.

5. Despite this red flag, Marriott International failed to sufficiently investigate Starwood's cybersecurity, leaving its guests exposed to cybercriminals for three more years. Marriott International did not detect the Starwood Breach until September 10, 2018.

6. The scope of the Starwood Breach is staggering in and of itself, but Marriott's failure to implement reasonable cybersecurity safeguards to protect guests' Personal Information is particularly egregious. Marriott failed to detect and report publicly hackers' presence in

---

Starwood rewards information (including points and balance), arrival and departure information, reservation date and the user's communication preferences.

Starwood's systems for *four years*, even though it had reported previous cybersecurity incidents during the same period. Marriott International's failure to adequately investigate Starwood's cybersecurity before the merger closed, and ongoing failure to take steps to protect its guests' personal information in the years following the merger, has permanently and irrevocably endangered the credit, identity, and safety of 500 million Starwood guests.

7. The Starwood Breach exposed an unprecedented range of Personal Information which may be exploited by cybercriminals to devastating effect. For example, passport numbers, when combined with some other forms of Personal Information exposed by Marriott, can be used to access individual travel histories through the United States Department of Homeland Security website, or leveraged to acquire real identity documents using stolen information, bypassing anti-counterfeiting measures.

8. Had Marriott's guests known that its cybersecurity was inadequate and that their information was exposed, many guests, including Plaintiff Taylor, would have chosen other lodgings, and would have changed the type of information provided to Marriott.

9. Even today, Marriott has not affirmatively and definitively notified all the individuals whose personal data has been compromised. As a result, hundreds of millions of Marriott's customers have not been informed that they should take steps to protect themselves because they are victims of hackers. Marriott's guests have not known to take freeze and monitor their credit, purchase dark web monitoring, or even take advantage of the few services Marriott has offered in the wake of the Starwood Breach. And, given the possibility that the Starwood Breach is part of an espionage campaign, without accurate information regarding the type of information stolen for each guest, guests cannot even begin to gauge the risks Marriott has

exposed them to by failing to secure their Personal Information. Marriott's failure to warn its customers, or to provide remediation to the extent possible, is indefensible.

10. As a result of Marriott's numerous failures, including its failure to implement reasonable cybersecurity measures to protect Personal Information, failure to take action to prevent or halt the penetration of its guest database, failure to disclose to guests that their Personal Information was not protected by adequate cybersecurity measures, and failure to provide timely and adequate notice of the Starwood Breach, affected guests have suffered numerous injuries, including the highly increased and ongoing risk of identity theft and unauthorized access to their most important online accounts; the costs associated with the time spent to understand, address, and attempt to protect themselves from the negative consequences resulting from the Starwood Breach; the stress, nuisance, and annoyance of navigating the potential consequences of the Starwood Breach without adequate notice from Marriott; the diminution in value of their Personal Information; and the loss of the use of funds expended through payment for lodging that Marriott falsely advertised as secure. Affected guests will require years of ongoing monitoring and remediation.

11. Plaintiff brings this class action to seek damages, injunctive and declaratory relief, the establishment of a fund to ensure that affected customers will be protected through ongoing monitoring and remediation services, and other relief pursuant to state privacy and tort laws related to an unprecedented data breach.

JURISDICTION AND VENUE

12. As set forth herein, this Court has general jurisdiction over Marriott and original jurisdiction over Plaintiff's complaint.

13. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in

controversy exceeds the sum of $5,000,000, and Marriott International and Starwood are each a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

14. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Marriott International's principal place of business is in this District and substantial parts of the events or omissions giving rise to the claims occurred in the District. Venue is also proper in the Greenbelt Division because Marriott is located here and the causes of action arose here.

THE PARTIES

15. Plaintiff Bonnie Taylor is a resident of California. Plaintiff has been a Starwood guest numerous times before September 10, 2018, the day Marriott claims it stopped the Starwood Breach. Plaintiff discovered that she was likely affected by the Starwood Breach after reading a news article reporting the breach on or around November 30, 2018. Plaintiff is at elevated risk of identity theft and loss due to Marriott's and Starwood's actions, and has spent time and effort seeking to remedy the harm caused by Marriott and Starwood.

16. Defendant Marriott International, Inc. is a Delaware corporation headquartered in Bethesda, Maryland. Following its acquisition of Starwood, Marriott became the world's largest lodging company, with more than 6,500 properties in 130 countries and territories, operating under 30 brands, including Marriott, Ritz-Carlton, W Hotels, Sheraton, St. Regis, and Le Méridien.[3] Marriott is Starwood's parent company.

[3] In 1998, Marriott bought The Ritz-Carlton Hotel Company and rights to the Ritz-Carlton hotel chain worldwide. The Ritz-Carlton Hotel Company now operates as an independently operated division of Marriott. Chris McGinnis, *Date Set for Big Marriott-Starwood-Ritz Program Merger*, S.F. CHRONICLE (July 26, 2018), https://www.sfgate.com/chris-mcginnis/article/Date-set-for-big-Marriott-Starwood-Ritz-program-13105658.php.

17. Defendant Starwood Hotels & Resorts Worldwide, LLC is a Maryland limited liability company headquartered in Stamford, Connecticut. Since September 2016, Starwood has been a subsidiary of Defendant Marriott.

FACTUAL ALLEGATIONS

Background: Marriott's Acquisition of Starwood

18. On November 4, 2015, Marriott International and Starwood announced that they had entered into a $12.2 billion merger agreement and began the process of clearing pre-merger antitrust reviews and seeking shareholder approval.

19. On November 20, 2015, perhaps prompted by the impending merger, Starwood announced that the point of sale systems at properties in North America had been infected by malware for at least 8 months. At the time of the initial disclosure, Starwood officials claimed that only 12 properties had been infected, and that guest reservation and loyalty systems were not affected by the attack. Starwood later amended its report to indicate that nearly 100 properties were affected by the malware attack.[4]

20. On March 1, 2016, Marriott International and Starwood announced that the transaction had cleared pre-merger antitrust reviews in the United States and in Canada. The shareholder vote was scheduled for March 28, 2016, and it seemed like a done deal.

21. On March 14, 2016, Starwood announced that it had received a $13 billion competing bid from Anbang Insurance Group, a Beijing-based holding company whose subsidiaries include insurance, banking, and financial services entities. A bidding war followed, with Anbang and Marriott International submitting competing offers until on March 20, Marriott

[4] *Starwood Hotels & Resorts Locations Affected by Payment Card Security Issue*, https://www.starwoodhotels.com/Media/PDF/Corporate/Hotel_List.pdf (Jan. 22, 2016).

International prevailed with a $13.6 billion proposal. Shareholders of both Marriott International and Starwood approved the deal in April 2016. Still, the Starwood-Marriot transaction faced additional hurdles in China.

22. On August 8, 2016, Starwood and Marriott International announced that the Ministry of Commerce of the People's Republic of China ("MOFCOM"), the entity with antitrust clearance authority in China, had asked for additional time to review the deal. At the time, experts raised concerns that MOFCOM was using the antitrust review process to "extract assets, intellectual property, and intellectual information technology" from Marriott and Starwood.[5] MOFCOM cleared the transaction on September 20, 2016.

23. On September 23, 2016, Marriott International completed its acquisition of Starwood. Under the acquisition agreement, Marriott International agreed to assume all of Starwood's unknown liabilities, including those described in this Complaint.

24. Starwood remains active as a Maryland limited liability company headquartered in Connecticut. It is a subsidiary of Marriott International.

Marriott's Integration of Starwood's Systems

25. Shortly after Marriott International completed its acquisition of Starwood, news emerged that Marriott International had decided to migrate Starwood's systems to Marriott International's systems.

26. On August 18, 2018, nearly two years after the transaction closed, Marriott completed the merger of their loyalty programs and systems, thereby completing the merger of

[5] Deanna Ting, *Is China Holding the Marriot-Starwood Deal Hostage?*, SKIFT (Aug. 9, 2016), https://skift.com/2016/08/09/is-china-holding-the-marriott-starwood-deal-hostage/.

the two companies' systems, and marking the first time Starwood and Marriot began operating as one since the 2016 acquisition.

27. The Starwood Breach appears emblematic of the problems Marriott has encountered in its integration of Starwood. Just two days before Marriott revealed the breach, the Wall Street Journal reported on the "turbulence" of Marriot's efforts to combine the Marriott and Starwood loyalty programs. The newspaper reported that "there were some widespread issues that Marriott says 'were quickly prioritized for correction.' Most involved data conversion and software bugs."[6] Even today, Marriott is still unifying its Starwood and Marriott reservation systems and expects to complete that task by the end of 2018.

28. Despite the multi-year project of integrating Starwood and Marriott's systems, which began in 2016, Marriott failed to detect the Starwood Breach until September 2018, and further failed to notify guests that they may have been affected until November 20, 2018.

The Starwood Breach

29. On November 30, 2018, Marriott filed a Form 8-K ("8-K") with the U.S. Securities and Exchange Commission ("SEC"). The 8-K announced that Marriott had "issued a press release providing important information regarding a cybersecurity incident."
The "cybersecurity incident" is the Starwood Breach, the second-largest data breach in history. The Starwood Database contains the Personal Information of approximately 500 million guests, including some or all of the following Personal Information: the guest's name, postal address, phone number, date of birth, gender, email address, passport number, encrypted credit card data, Starwood rewards information (including reward points and balance, and possibly the customer's

[6] Scott McCartney, *Inside the Marriott-Starwood Loyalty Program Turbulence,* WALL ST. J. (Nov. 28, 2018), https://www.wsj.com/articles/inside-the-marriott-starwood-loyalty-program-turbulence-1543416010.

log-in and password, detailed hotel stay history, favorite hotels, room preferences, her linked Facebook account, and more), arrival and departure information, reservation dates, and the user's communication preferences.

30. Marriott said an internal security tool alerted it to a potential breach on September 8, 2018. After an investigation, the company found that the Starwood Database may have been compromised since 2014. The Starwood Database contained information for guests who made reservations on or before September 10, 2018, at Starwood hotels globally.

31. For approximately 327 million of those guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

32. For some of those 327 million guests, the Personal Information also includes encrypted payment card numbers and payment card expiration dates. There are two components needed to decrypt the payment card numbers, and as of its November 30, 2018 8-K, Marriott has not been able to rule out the possibility that hackers stole both of those components.

33. For the remaining 173 million guests in the Starwood Database, the Personal Information was limited to the guest's name and sometimes other data, such as the guest's mailing address, email address, and other information that Marriott has not yet identified.

34. Marriott's press release included this quote from Marriott Chief Executive Arne Sorenson: "We fell short of what our guests deserve and what we expect of ourselves,", but Marriott did not make company executives available for interviews on the day Marriott announced the breach.

Numerous Government Entities Are Conducting Ongoing Investigations of the Starwood Breach

35. Numerous regulators in the U.S. and abroad are investigating. A Federal Bureau of Investigation spokeswoman said the agency is tracking the situation and as of the filing of this Complaint, attorneys general in numerous states, including Maryland, New York, Illinois, Massachusetts, Pennsylvania, and Texas, had opened investigations.

36. Marriott will face scrutiny from regulators in Europe, where the European Union's General Data Protection Regulation privacy law took effect in May 2018. Although the original penetration of the Starwood Database appears to predate the GDPR, the incident is likely be subject to the law because the unauthorized activity, including Marriott's detection of an unauthorized access attempt, continued after the law went into effect.

37. Britain's Information Commissioner's Office, which can fine companies for failing to protect customers' personal data, is also investigating the Starwood Breach. Due to the number of government investigations in the United States and abroad, additional details about the Starwood Breach are likely to emerge.

38. Marriott claims it is still "in the dark about a lot of what happened." Marriott CEO Arne Sorenson told U.S. Representative for Maryland Jamie Raskin of the hackers, "It could be a criminal gang, it could be a foreign government, it could be almost anybody."[7]. Two people briefed on the U.S. government's investigation of the Starwood Breach have said that investigators increasingly believe that Chinese hackers working on behalf of the Ministry of

[7] *Dem lawmaker: Marriott 'in the dark' about massive data breach*. The Hill, https://thehill.com/policy/cybersecurity/419549-dem-lawmaker-marriott-in-the-dark-about-massive-data-breach

State Security, China's civilian spy agency, were most likely responsible for the breach.[8] The hack of Starwood's system is believed to be part of a Chinese intelligence-gathering effort that also hacked health insurers and the security clearance files of millions more Americans.

39. The people familiar with the investigation said the Marriott breach involved the same cloud-hosting space that Chinese state hackers have used in the past, and that one signature technique that involved hopping among servers also points to Chinese involvement. Another clue suggesting nation-state involvement was that none of the breached data has appeared on the dark web or any of the forums that criminals typically use to sell stolen credentials and other valuable personal data.

40. As discussed below, the Personal Information stolen in the Starwood Breach can be aggregated with other stolen information, making victims of data breaches vulnerable to increasingly sophisticated levels of identity theft, financial crimes, and other forms of fraud. This aggregated information is valuable to criminals seeking to commit identity fraud and to intelligence agencies seeking to build dossiers and track movements of diplomats, spies, military personnel, business executives and journalists, according to several cybersecurity experts.

Marriott Knew Its Systems Were Vulnerable

41. Marriott said an internal security tool alerted it to a potential breach nearly three months ago, on September 8, 2018, as Marriott completed the integration of its Starwood and Marriott guest information systems. Marriott's subsequent investigation revealed that there had been unauthorized access to the Starwood Database since 2014, and that the hackers had tried to remove the guest information using an encrypted file.

[8] David E. Sanger et al., *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. TIMES (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

42. However, in 2015, shortly after the Marriott-Starwood merger was announced, Starwood disclosed an eight-month-long data breach at numerous Starwood locations that resulted in the theft of payment card information. In that breach, attackers installed malware on point-of-sale systems in approximately 100 hotel restaurants and gift shops to siphon off payment card information.[9] In a January 22, 2016 letter addressing the incident, Starwood's then-President promised that "protecting the security of our customers' personal information is a top priority for Starwood" and indicated that the Starwood guest reservation and membership systems were not affected.[10]

43. Cybersecurity specialists agree that a more thorough investigation into the 2015 intrusion likely would have uncovered the attackers, who instead were able to lurk in the Starwood Database for three more years.[11]

44. Marriott's failure to discover the Starwood Breach during its acquisition due diligence or post-acquisition systems integration suggests that Marriott did not sufficiently analyze or evaluate Starwood's cybersecurity system, instead focusing on Marriott's legacy

[9] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, WALL ST. J. (Dec. 2, 2018), https://www.wsj.com/amp/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

[10] *Letter From Our President – Updated*, Starwood Hotels (Jan. 22, 2016), https://www.starwoodhotels.com/html/HTML_Blocks/Corporate/Confidential/Letter.htm?EM=VTY_CORP_PAYMENTCARDSECURITYNOTICE.

[11] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, WALL ST. J. (Dec. 2, 2018), https://www.wsj.com/amp/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

system and integration, leaving Starwood's database vulnerable.[12] Marriott's failure to perform adequate due diligence has caused serious, ongoing harm to Marriott customers.

45. Marriott's representatives did not respond to Law360's December 3, 2018 request to explain what level of cybersecurity research it conducted before finalizing its acquisition of Starwood.[13]

46. Moreover, there are reports that Starwood and Marriott have experienced other breaches that they failed to disclose. Forbes reports that Marriott's own Cyber-Incident Response Team (CIRT) had been affected.[14]

47. Marriott knew that its own systems were vulnerable and that it needed to dedicate more resources to the problem of hacking. On July 1, 2017, MalwareHunterTeam, an independent cybersecurity research group that intercepts and analyzes malware, intercepted a message, from a malware-infected machine to the malware's "command and control" server. MalwareHunterTeam saw a screenshot of the infected machine, which belonged to a Marriott CIRT employee and, according to MalwareHunterTeam, was likely Marriott's main CIRT account.[15] CIRT accounts are particularly valuable to compromise given their importance to

---

[12] Israel del Rio-Quilmach, *I Was a Senior VP of Technology at Starwood—Here's My Take on the Guest Data Breach*, PHOCUSWIRE (Dec. 10, 2018), https://www.phocuswire.com/Marriott-data-breach-ex-Starwood-perspective.

[13] Ben Kochman, *Marriott Hack Shows Risks Of Lax Cyber Diligence In Mergers*, LAW360 (Dec. 3, 2018), https://www.law360.com/cybersecurity-privacy/articles/1106916/marriott-hack-shows-risks-of-lax-cyber-diligence-in-mergers

[14] Thomas Brewster, *Revealed: Marriott's 500 Million Hack Came After a String of Security Breaches*, FORBES (Dec. 3, 2018), https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches.

[15] @malwrhunterteam, TWITTER (July 1, 2017, 2:57 AM), https://twitter.com/malwrhunterteam/status/881089396124078080.

companies' efforts to protect themselves from cyberattack, and CIRT hacks are difficult to recover from, because they so frequently include information regarding company cybersecurity features.

Marriott Failed to Timely Inform Affected Guests

48. By November 19, 2018, Marriott had decrypted the information and determined that the stolen data was guest data from the Starwood Database. Yet Marriott failed to notify its customers of the breach until November 30, 2018, and as of the date of the filing of this complaint, Marriott has not affirmatively and definitively notified any or all specific individuals that their personal data has been compromised. Marriott's failure to warn its customers, or to provide remediation to the extent possible, is indefensible.

49. On November 30, 2018, Marriott claimed it would begin notifying affected guests whose email addresses were in the Starwood database.

50. To the detriment of Marriott's own customers, the website Marriott set up for Starwood customers, titled "Starwood Guest Reservation Database Security Incident,"[16] does not allow customers to check if their Personal Information was stolen during the Starwood Breach. In response to "Was my information involved?" in the Frequently Asked Questions portion of the website, Marriott states only, "If you made a reservation on or before September 10, 2018 at a Starwood property, information you provided may have been involved. You may choose to enroll in WebWatcher if it is available in your country. Guests from the United States who enroll in WebWatcher will also be provided fraud consultation services and reimbursement coverage free of charge."

[16] https://answers.kroll.com/

Repercussions of the Starwood Breach for Customers

51. The Starwood Breach is the second-largest data breach in history. Based on the number of individuals Marriott has identified as potentially affected, security analysts have stated that only Yahoo's breach in 2013—impacting three billion people, or nearly the entirety of Yahoo's user base—may be bigger.

52. Due to the large number of data breaches just in the last year,[17] cybercriminals can both aggregate stolen information and cross check it with publicly available information to assemble information that can be leveraged to not only gain access to financial accounts, but to steal identities.

53. Hacks have proliferated across the hospitality industry. Security analysts say the industry is a ripe target for criminal actors because of the wealth of financial and other information flowing through payment and reservation systems. Hotels often have multiple cards on file for their frequent guests. In addition, frequent business travelers incur many charges on work-related trips and may be slow to spot unusual transactions on credit cards that are used solely or partially for work. And, as discussed below, infrequent travelers may not be aware that their identity has been stolen and used to obtain travel documents in their name.

[17] According to Gates Marshall, director of cyber services for the information security and consulting firm Compliance Point, roughly 800 million personal records were compromised in November 2018 alone. According to Privacy Rights Clearinghouse, approximately 11 billion personal records have been exposed in breaches since 2005.

Injuries Related to Stolen Passport Numbers

54. Security analysts say the range of customer data potentially compromised—such as passport numbers, travel details and payment-card data—make the breach even more sensitive.

55. "There is a risk that these passport numbers can be paired with other useful identifiers," such as social security numbers, home addresses and email password-security answers, said David Weinstein, vice president of threat research at security firm Claroty and a former official at U.S. Cyber Command. Mr. Weinstein said he wasn't aware of any previous theft of so many passport numbers.

56. As U.S. Senator Charles Schumer summarized, "The experts will tell you, there is an art to identity theft and it lies in the ability to paint the most complete picture of the person whose information you're looking to steal or sell. Unfortunately, for many travelers who have stayed in one of Marriott's Starwood hotels, they've provided the company with an array of personal color—like their passport information—that thieves can now access to complete the canvass and assume or sell an identity."[18]

57. "Passport data is something you should hold onto more tightly than something like a driver's license," said Pam Dixon, executive director of the World Privacy Forum, a nonprofit public interest research group focused on privacy and security. "The biggest problem is that if someone is able to get a passport with your identity, they can cross jurisdictions. The

[18] Taylor Telford, *Schumer: Marriott Should Pay for New Passports Compromised by Data Breach,* WASH. POST (Dec. 3, 2018), https://www.washingtonpost.com/business/2018/12/03/schumer-marriott-should-pay-new-passports-compromised-by-data-breach.

nightmare scenario is that you travel overseas and someone has committed a crime there in your name."[19]

58. Fake passports have been a best-selling item on the black market for decades. A fake U.S. document sell for up to $4,000 and beyond for a criminal who wants to impersonate a U.S. citizen domestically or when traveling abroad. A passport can provide a second form of ID typically required for opening accounts or proving residence.

59. One way for criminals to obtain a fake passport is to use personal data to apply online for a new one by reporting the old one lost or stolen. The application process for a new passport is relatively simple. It requires filling out a form that is similar to a sign-up for a new streaming service or a purchase—with a few extra requirements.

60. Mark Weiner from security firm Balbix stated, "With your passport number, name, and date of birth, anyone can apply for a new passport by reporting the existing one stolen, use it as a proof of identity to open a new bank account or access an existing one. Your passport number is an integral part of your identity, along with your name and date of birth and it can cause immense damage in the wrong hands."[20]

61. The most challenging part for a criminal re-applying for a fraudulent passport is having a social security number for the victim, but Equifax leaked millions of those earlier this year. Beyond that, everything needed was potentially part of the Personal Information stolen in the Starwood Breach or available in a bundle of identity information sold on the dark web.

---

[19] *The Marriott Data Breach Exposed Millions of Passports. Here's What Thieves Can Do with Them*, POPULAR SCI. (Nov. 30, 2018), https://www.popsci.com/passport-number-hacked-marriott.

[20] Kari Paul, *Exclusive: After Massive Hack, Marriott Pledges to Pay for New Passports if Fraud Has Taken Place*, MARKETWATCH (Dec. 4, 2018), https://www.marketwatch.com/story/after-massive-hack-marriott-pledges-to-pay-for-new-passports-if-fraud-has-taken-place-2018-12-03.

62. The amount of biometric protection baked into passports customs systems around the world—as well as compatible airports and other travel facilities—has climbed substantially, but techniques for fooling biometrics systems have already popped up to help fake passports more useful for illicit behavior.

63. One technique to pass biometric tests of fake documents is called morphing. It is a process that involves using image editing techniques to combine the face of the victim with the face of the criminal into an amalgamation that's close enough to get by basic face scanning or, even easier, a simple visual once-over from a human guard. Morphing is the driving force behind the black market for selfies on the dark web.

64. Criminals in possession of a stolen passport number can easily obtain an individual's international travel history directly from the United States federal government. According to the Department of Homeland Security, Americans can track their international travel using an online tool that is available to the public. It requires the person's full name, birthday, and passport number, all of which were part of the Starwood Breach.

65. Information gleaned from the Department of Homeland Security's online tool is gold for hackers trying to pick the best victims. "If you're the type of traveler who doesn't go many places and keeps your passport in the drawer, that might make you a great target," said Pam Dixon, executive director of the World Privacy Forum. "It decreases the odds someone will notice the fraud."

66. In addition, the passport information could be especially valuable to state actors looking to compile detailed dossiers on international business travelers and government officials.

67. Class members whose passport numbers were stolen will be forced to apply for a new passport at a cost ranging from of $110 to $170, according to the U.S. State Department website.

Other Injuries from Data Stolen During the Starwood Breach

68. A company that partnered with Starwood and booked business travel with Starwood would now be more vulnerable to other hackers if the Starwood Breach hackers stole the data of many employees of the company, and will incur costs associated with, among other things, issuing new corporate travel credentials and monitoring its own systems.

69. As Paige Boshell of law firm Privacy Counsel LLC explained, "If you think about why Starwood was so attractive to Marriott, it's very high-end and has loyal guests that travel frequently, including senior executives and the other key people at an organization. So businesses that have very valuable proprietary or business information and have a senior executive visiting Starwood hotels in different countries need to be mindful that their patterns may be able to be tracked and used to target or impersonate senior executives later."[21]

70. Marriott properties are also frequently used by the federal government for travel purposes, meaning that the hackers may have been able to track the under-the-radar movements and activities of government officials since as far back as 2014.[22]

---

[21] Allison Grande, *Marriott Hack Shows High Premium Placed on Travel Details*, LAW360, https://www.law360.com/cybersecurity-privacy/articles/1106584/marriott-hack-shows-high-premium-placed-on-travel-details.

[22] Allison Grande, *Marriott Hack Shows High Premium Placed on Travel Details*, LAW360, https://www.law360.com/cybersecurity-privacy/articles/1106584/marriott-hack-shows-high-premium-placed-on-travel-details; David E. Sanger et al., *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. TIMES (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

71. Because of the Starwood Breach, Plaintiff and Class members are more susceptible to burglaries. Rusty Carter, vice president of Arxan Technologies, a San Francisco-based company, said that criminals working with hackers could track the travel plans of victims. As Carter explained, "If I know where you live, which is captured in the billing address, and I know where you're going to be and when, there is potential [to burglarize your house]."[23]

72. The Starwood Breach puts Plaintiff and Class members at a higher risk of tax fraud. Criminals with Plaintiff's and Class members' stolen information could file fraudulent claims in the victims' names and collect the victims' tax refunds.

73. Plaintiff and Class members are also at a much higher risk of identity theft due to the Starwood Breach.

74. Experts recommend that Starwood customers such as Plaintiff freeze their credit immediately to protect against identity theft.[24] Paige Boshell, a privacy and cybersecurity attorney with the law firm Privacy Counsel LLC in Birmingham, Alabama, told USA Today, "The potential damage cannot be understated. This type of information may be retained and used over and over again for years."[25] Franklyn Jones, Chief Marketing Officer of Cequence Security, similarly told USA Today, "The unfortunate thing is the impact is just getting started. What

---

[23] Tim Johnson, *Hackers Lurked Undetected on Networks Now Owned by Marriott for 4 Years*, SACRAMENTO BEE (Nov. 30, 2018), https://www.sacbee.com/news/nation-world/national/article222437465.html.

[24] Gary Stoller, *Freeze Your Credit Now After Marriott/Starwood Hacking, Expert Says*, FORBES (Dec. 3, 2018), https://www.forbes.com/sites/garystoller/2018/12/03/freeze-your-credit-now-after-marriottstarwood-hacking-expert-says.

[25] Anika Reed, *Marriott Data Breach: Class-Action Suit Filed; Experts Ask Why It Wasn't Caught Earlier*, USA TODAY (Dec. 3, 2018), https://www.usatoday.com/story/travel/news/2018/12/03/marriott-data-breach-lawsuit-filed-2015-breach-prompts-questions/2190708002/.

typically happens from these breaches is that the data finds its way out to the dark web, and bad people find those stolen credentials and try them on other websites to see if they can get them into other accounts."[26] David Ginsburg, vice president of marketing at Cavirin, a California-based provider of cybersecurity risk posture and compliance, stated, "[W]e need to finally address the fact that all personal data is at risk and will be used by hackers to build complete profiles of individuals that may be monetized."[27]

CLASS ALLEGATIONS

75. Plaintiff brings this proposed action pursuant to Federal Rules of Civil Procedure ("Rules") 23(a) and 23(b)(2), and/or (b)(3) on behalf of itself and as a class action, seeking injunctive relief and damages on behalf of the following nationwide class of those similarly situated:

> **All persons whose Personal Information was compromised in the Starwood Breach ("Nationwide Class").**

76. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of California state law claims in the alternative to the nationwide claims brought under Maryland common law, as well as statutory claims under California state data breach statutes and consumer protection statutes on behalf of a separate statewide subclass for California, defined as follows:

---

[26] Anika Reed, *Marriott Data Breach: Class-Action Suit Filed; Experts Ask Why It Wasn't Caught Earlier*, USA TODAY (Dec. 3, 2018), https://www.usatoday.com/story/travel/news/2018/12/03/marriott-data-breach-lawsuit-filed-2015-breach-prompts-questions/2190708002/.

[27] Kari Paul, *Exclusive: After Massive Hack, Marriott Pledges to Pay for New Passports if Fraud Has Taken Place*, MARKETWATCH (Dec. 4, 2018), https://www.marketwatch.com/story/after-massive-hack-marriott-pledges-to-pay-for-new-passports-if-fraud-has-taken-place-2018-12-03.

All natural persons residing in California whose Personal Information was compromised as a result of the Starwood Breach ("California Subclass").

77. Excluded from the Classes are Marriott; officers, directors, and employees of Marriott; any entity in which Marriott has a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of Marriott.

78. Plaintiff is a member of the Class.

79. Marriott's conduct has caused injury to Class members.

80. The Class members are so numerous that joinder of all members is impracticable, as approximately 500 million individuals' Personal Information may have been compromised.

81. The Class members are readily ascertainable and can easily be identified by records maintained by Defendant. Notice can be provided by means permissible under the Federal Rules of Civil Procedure.

82. There are substantial questions of law and fact common to the Classes. These questions include, but are not limited to, the following:

(a) Whether Marriott failed to provide adequate security and or protection for its computer systems containing Plaintiff's and members of the potential Classes' financial and personal data;

(b) Whether Marriott's conduct resulted in the unauthorized breach of its computer systems containing Plaintiff's and members of the potential Classes' financial and personal data;

(c) Whether Marriott disclosed (or directly or indirectly caused to be disclosed) private financial and personal information of Plaintiff and members of the potential Class;

(d) Whether Marriott owed a legal duty to Plaintiff and members of the potential Class to use reasonable care regarding their personal information;

(e) Whether Marriott unreasonably delayed in announcing the Starwood Breach;

(f) Whether Marriott breached its duties to exercise reasonable due care in obtaining, using, retaining, and safeguarding Plaintiff's and members of the potential Classes' Personal Information;

(g) Whether Marriott was negligent;

(h) Whether Marriott's breach of its duties proximately caused damages to Plaintiff and other Class members;

(i) Whether Marriott has breached its duty to maintain the privacy of Plaintiff's and Class members' information;

(j) Whether Plaintiff and Class members have suffered damages, including an increased risk of identity theft as a result of Marriott's failure to protect Plaintiff's and Class members' Personal Information; and

(k) Whether Plaintiff and other Class members are entitled to compensation, damages, and/or other relief as a result of the breach of duties alleged herein.

83. Plaintiff's claims are typical of the claims of all Class members. The same events and conduct that give rise to Plaintiff's claims and legal theories also give rise to the claims and legal theories of the Classes. Specifically, Plaintiff's and Class members' claims arise from

Marriott's failure to install and maintain reasonable security measures to protect Plaintiff's and Class members' Personal Information.

84. Marriott has acted and refused to act on grounds generally applicable to the Classes described herein.

85. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Marriott.

86. Plaintiff will fairly and adequately represent the interests of the Classes. There are no disabling conflicts of interest between Plaintiff and the Classes.

87. Plaintiff is represented by experienced counsel who are qualified to litigate this case. The lawsuit will be capably and vigorously pursued by Plaintiff and her counsel.

88. A class action is superior to other available methods for a fair and efficient adjudication of this controversy since joinder of all Class members is impracticable.

89. The damages suffered by individual Class members may be relatively small in comparison with the expense and burden associated with individual litigation, which make it impossible for them to individually redress the harm done to them.

90. Proceeding as a class action will permit an efficient administration of the claims of Class members. Class treatment of these claims will save time, ensure uniformity in factual and legal rulings, and allows all parties to conserve legal fees that would otherwise be expended in litigating common issues piecemeal.

CLAIMS FOR RELIEF[28]

COUNT I

VIOLATION OF MARYLAND CONSUMER PROTECTION ACT, MD. CODE ANN. COMM. LAW § 13-301 *ET SEQ.*

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and All Class Members)

91. Plaintiff, individually and on behalf of all Class members, restates and realleges the foregoing allegations as if fully set forth herein.

92. This claim for relief is brought pursuant to the Maryland Consumer Protection Act, Md. Code Ann., Comm. Law § 13-101 *et seq.* ("MCPA").

93. Plaintiff and all Class members are consumers under the MCPA who transacted with and provided Personal Information to Defendants.

94. Defendants, as legal or commercial entities, are "persons" under the MCPA.

95. Defendants are also merchants under the MCPA. Defendants offer or make available to consumers hotel rooms and related goods and services, which are goods or services that are primarily for personal, household, or family purposes under MCPA § 13-101(d).

96. At all relevant times, Marriott International has maintained its principal place of business in the State of Maryland and has regularly conducted business throughout the State. Starwood was formed in the State of Maryland and has regularly conducted business throughout the State.

97. MCPA prohibits unfair, abusive, or deceptive trade practices. Defendants have violated the MCPA in at least the following ways:

[28] References to "Marriott" in these causes of action include Marriott's subsidiary, Starwood, where appropriate.

(a) by failing to implement, test and maintain appropriate cybersecurity measures;

(b) by failing to protect and safeguard the Personal Information of Plaintiff and Class members from being lost, stolen, compromised, misused and/or disclosed to unauthorized users;

(c) by failing to timely disclose to Plaintiff and Class members that their Personal Information was compromised, lost, stolen, misused and/or disclosed to unauthorized parties and precisely the type of information compromised; and

(d) by violating the Maryland Code, Commercial Law § 14-3501, *et seq.*

98. Defendants have engaged in unfair, abusive, or deceptive trade practices within the meaning and in violation of the MCPA because:

(a) Defendants' wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures are substantially injurious to Plaintiff and Class members, offend public policy, and/or are unfair, immoral, abusive, unethical, oppressive, deceptive and/or unscrupulous;

(b) any justification for Defendants' conduct would be outweighed by the gravity of the injury to Plaintiff and Class members;

(c) there were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct; and

(d) Defendants' conduct violates common and statutory law as alleged herein, including Maryland Code, Commercial Law § 14-3501, *et seq.*

99. Defendants further violated MCPA § 13-301(2) by representing to consumers that their consumer goods and consumer services were of a particular standard, quality, grade, style, or model which they are not.

100. Defendants further violated MCPA § 13-301(3) by failing to state a material fact. That failure deceived or tended to deceive consumers. Defendants' misconduct, nondisclosures, and misleading statements were false, misleading, and likely to deceive Plaintiff and Class members in violation of the MCPA.

101. Defendants violated MCPA § 13-301(9) by deception, fraud, false pretense, false premise, misrepresentation, knowing concealment, suppression, and/or omission of material facts, with the intent that Plaintiff and Class members rely on the same, relating to the collection, retention, and safeguarding of Personal Information in connection with the lease of hotel rooms.

102. Defendants' misrepresentations and fraudulent omissions were material to Plaintiff and Class members. Plaintiff and Class members would not have provided their Personal Information to Defendants if Defendants had disclosed that it would not adequately protect and safeguard their Personal Information from access by unauthorized users, including hackers.

103. As a direct and proximate result of Defendants' unlawful, unfair, and/or fraudulent conduct in violation of the MCPA, Plaintiff and Class members have suffered injury in fact and will continue to be injured. Further, as a direct and proximate result of Defendants' violation of the MCPA, Plaintiff and Class members incurred actual damages, including, *inter*

alia, expenses associated with monitoring their Personal Information to prevent identity theft and/or fraud.

104. As a result of Defendants' unfair and deceptive trade practices, Plaintiff and members of the Class demand judgment against Defendants for restitution, disgorgement, statutory and actual monetary damages, interest, costs, attorneys' fees and injunctive relief, including a declaratory judgment and an appropriate court order prohibiting Defendants from further deceptive acts and practices described in this complaint.

COUNT II

Violation of California Customer Records Act, Cal. Civ. Code § 1798.81.5

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and the California Subclass)

105. Plaintiff, individually and on behalf of the California Subclass, restates and realleges the foregoing allegations as if fully set forth herein.

106. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted the California Customer Records Act ("CRA"), Cal. Civ. Code § 1798.80–1798.84, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

107. Plaintiff and Class members bring this claim pursuant to California Civil Code § 1798.81.5, a provision of the CRA that allows customers to recover damages in the event of a data breach due to a company's inadequate security.

108. Marriott International and Starwood are businesses that own, maintain, and/or license personal information, within the meaning of California Civil Code § 1798.81.5, about California residents Plaintiff and California Subclass members.

109. Plaintiff and California Subclass members provided personal information to Defendants for the purpose of purchasing or leasing a product or obtaining a service from Defendants.

110. The Personal Information that Plaintiff and California Subclass members provided to Defendants is defined as "personal information" under California Civil Code § 1798.82(d)(1).

111. Defendants' inadequate security practices failed to protect Plaintiff and California Subclass members Personal Information from falling into unauthorized hands.

112. As a direct and proximate result of Defendants' unlawful, unfair, and/or fraudulent conduct in violation of California Civil Code § 1798.81.5, Plaintiff and Class members have suffered injury in fact and will continue to be injured. Further, as a direct and proximate result of Defendants' violation of the MCPA, Plaintiff and Class members incurred actual damages, including, *inter alia*, expenses associated with monitoring their Personal Information to prevent identity theft and/or fraud.

113. Plaintiff and California Subclass members seek relief under California Civil Code § 1798.84, including actual damages and injunctive relief.

COUNT III

Violation of California Customer Records Act, Cal. Civ. Code § 1798.82

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and the California Subclass)

114. Plaintiff, individually and on behalf of the California Subclass, restates and realleges the foregoing allegations as if fully set forth herein.

115. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted the California Customer Records Act ("CRA"), Cal. Civ. Code § 1798.80–1798.84, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

116. Plaintiff and Class members bring this claim pursuant to California Civil Code § 1798.82, a provision of the CRA that allows customers to recover damages in the event of delayed notification of a data breach.

117. Plaintiff and California Subclass members provided personal information to Defendants for the purpose of purchasing or leasing a product or obtaining a service from Defendants.

118. The Personal Information that Plaintiff and California Subclass members provided to Defendants is defined as "personal information" under California Civil Code § 1798.82(d)(1).

119. Marriott International and Starwood conduct business in California.

120. Marriott International and Starwood are businesses that own, maintain, and/or license computerized data that includes personal information, within the meaning of California Civil Code § 1798.81.5, about California residents Plaintiff and California Subclass members.

121. A data breach of Starwood compromised Plaintiff's and California Subclass members' personal information within the meaning of California Civil Code § 1798.81.5.

122. Marriott is therefore required to notify California residents Plaintiff and California Subclass members "(1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable." Cal. Civ. Code § 1798.82(a).

123. Marriott is required to make this disclosure "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82.

124. Among other requirements, Marriott's security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

125. Because Marriott knew or reasonably believed that Plaintiff's and California Subclass members' personal information was acquired by unauthorized persons during the Starwood Breach, Marriott had an obligation to disclose the Starwood Breach in a timely and accurate fashion as mandated by California Civil Code § 1798.82.

126. By failing to disclose the Starwood Breach in a timely and accurate manner, Defendants violated California Civil Code § 1798.82.

127. As a direct and proximate result of Marriott's delayed data breach notification in violation of California Civil Code § 1798.82, Plaintiff and Class members have suffered injury in fact and will continue to be injured.

128. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT IV

Violation of the California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and the California Subclass)

129. Plaintiff, individually and on behalf of the California Subclass, restates and realleges the foregoing allegations as if fully set forth herein.

130. The Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750–1784, is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

131. Marriott International and Starwood are "persons" as defined by Civil Code §§ 1761(c) and 1770 and have provided "services" as defined by Civil Code §§ 1761(b) and 1770.

132. Plaintiff and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

133. Defendants' acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade when they were not;

(c) Advertising goods or services with intent not to sell them as advertised; and

(d) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

134. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

135. Had Defendants disclosed to Plaintiff and Class members that Starwood's data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as one of the world's largest hotel companies and was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the California Subclass. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Accordingly, because Marriott held itself out as having a special role in the hotel industry with a corresponding duty of trustworthiness and care, Plaintiff and the

California Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

136. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

137. Plaintiff and the California Subclass have provided notice of their claims for damages to Marriott, in compliance with California Civil Code § 1782(a).

138. Plaintiff and the California Subclass seek all monetary and nonmonetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT V

California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and the California Subclass)

139. Plaintiff, individually and on behalf of the California Subclass, restates and realleges the foregoing allegations as if fully set forth herein.

140. Defendants violated California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.*, by engaging in unlawful, unfair, and deceptive business acts and practices.

141. Marriott International and Starwood are "persons" as defined by California Business and Professions Code § 17201.

142. Defendants' "unfair" acts and practices include:

(a) Defendants' failure to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Starwood Breach. Marriott failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Personal Information has been compromised.

(b) Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §§ 41-58), the Gramm-Leach-Bliley Act ("GBLA") (15 U.S.C. §§ 6801-6809), and the California Customer Records Act ("CRA") (Cal. Civ. Code §§ 1798.80–1798.84).

(c) Defendants' failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Marriott's

inadequate security, consumers could not have reasonably avoided the harms that Marriott caused.

(d) Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

143. Defendants have engaged in "unlawful" business practices by violating multiple laws, including the California CRA (Cal. Civ. Code §§ 1798.80–1798.84), the California CLRA (Cal. Civ. Code §§ 1750–1784), the Fair Credit Reporting Act ("FCRA") (15 U.S.C. §§ 1681–1681x), the GBLA (§§ 6801-6809), the FTC Act (15 U.S.C. §§ 41-58), and California common law.

144. Defendants' unlawful, unfair, and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass members' Personal Information, which was a direct and proximate cause of the Starwood Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Starwood Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' Personal Information, including duties imposed by the FTC Act (15 U.S.C. §§ 41-58), the FCRA (15 U.S.C. §§ 1681–1681x), the GBLA (§§ 6801-6809), and the California CRA (Cal. Civ. Code §§ 1798.80–

1798.84), which was a direct and proximate cause of the Starwood Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' Personal Information, including duties imposed by the FTC Act (15 U.S.C. §§ 41-58), the FCRA (15 U.S.C. §§ 1681–1681x), the GBLA (§§ 6801-6809), and the California CRA (Cal. Civ. Code §§ 1798.80–1798.84);

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and California Subclass members' Personal Information; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' Personal Information, including duties imposed by the FTC Act (15 U.S.C. §§ 41-58), the FCRA (15 U.S.C. §§ 1681–1681x), the GBLA (§§ 6801-6809), and the CRA (Cal. Civ. Code §§ 1798.80–1798.84).

145. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

146. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, including the costs passed through to Marriott from their transactions, the premiums and/or price received by Marriott for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

147. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass members' rights. Starwood's past data breach put Defendants on notice that their security and privacy protections were inadequate.

148. Plaintiff and California Subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT VI

Negligence

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and All Class Members)

149. Plaintiff, individually and on behalf of all Class members, restates and realleges the foregoing allegations as if fully set forth herein.

150. Defendants had a duty to exercise reasonable care to protect and secure Plaintiff's and Class members' Personal Information within its possession or control from being

compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This highly confidential Personal Information includes but is not limited to name, postal address, phone number, date of birth, gender, email address, passport number, encrypted credit card data, Starwood rewards information (including points and balance), arrival and departure information, reservation date and the user's communication preferences.

151. Defendants' duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class members' Personal Information in their possession was adequately secured and protected, and was retained only for legitimate purposes and with adequate storage, retention and disposal policies.

152. Marriott further had a duty to implement processes that would detect a breach of its security systems in a timely manner.

153. In light of the special relationship between Plaintiff and Class members and Defendants, whereby Defendants required Plaintiff and Class members to provide highly sensitive and confidential Personal Information as a condition of obtaining Defendants' services, Defendants undertook a duty of care to ensure the security of such information.

154. Through its acts or omissions, Defendants breached their duty to use reasonable care to protect and secure Plaintiff's and Class members' Personal Information within its possession or control. Defendants breached their duty by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class members' Personal Information, failing to adequately monitor the security of its network allowing unauthorized access to Plaintiff's and Class members' Personal Information, and failing to recognize in a timely manner that Plaintiff's and Class members' Personal Information had been compromised.

155. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and Class members, the Starwood Breach would not have occurred and Plaintiff's and Class members' Personal Information would not have been compromised.

156. The injury and harm suffered by Plaintiff and Class members were the reasonably foreseeable and probable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Personal Information in its possession or control. Marriott knew or should have known that its systems and technologies for processing and securing Plaintiff's and Class members' Personal Information had significant vulnerabilities.

157. As a result of Defendants' negligence, Plaintiff and Class members have incurred damages, and are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse.

COUNT VII

Negligence *Per Se*

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and All Class Members)

158. Plaintiff, individually and on behalf of all Class members, restates and realleges the foregoing allegations as if fully set forth herein.

159. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Marriott of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Marriott's duty.

160. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and failing to comply with

industry standards. Marriott's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach at one of the world's largest hotel chains.

161. Marriott's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

162. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

163. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Classes.

164. As a direct and proximate result of Marriott's negligence, Plaintiff and Class members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT VIII

Unjust Enrichment Based on Quasi-Contract

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and All Class Members)

165. Plaintiff, individually and on behalf of all Class members, restates and realleges the foregoing allegations as if fully set forth herein.

166. Plaintiff and Class members conferred a benefit on Defendants by staying at and paying for Starwood hotels and providing Personal Information to Defendants.

167. Plaintiff and Class members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Marriott and that was ultimately stolen in the Starwood Breach.

168. Marriott benefitted from Plaintiff's and Class members' payment for their stays in Starwood hotels and from Plaintiff's and Class members' Personal Information. Marriott also benefitted from its ability to retain and use Plaintiff's and Class members' Personal Information.

169. Marriott knew and appreciated that it was in fact so benefitted.

170. Marriott also knew and appreciated that the Personal Information pertaining to Plaintiff and Class members was private and confidential and its value depended upon Marriott maintaining the privacy and confidentiality of that Personal Information.

171. Plaintiff and Class members had the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class members reasonably believed that Defendants would use part of the monies they paid to Defendants for stays at Starwood hotels to fund adequate and reasonable data security practices.

172. But for Marriott's willingness and commitment to maintain the privacy and confidentiality of Plaintiff and Class members and provide timely and accurate notice in the event of a data breach, Plaintiff and Class members would not have given that Personal Information to Defendants. Further, if Defendants had disclosed that their data security measures were inadequate, they would not have been permitted to continue in operation by regulators, its shareholders, and participants in the marketplace.

173. As a result of Marriott's wrongful conduct as alleged in this Complaint (including among things its utter failure to employ adequate data security measures, its continued

maintenance and use of the Personal Information belonging to Plaintiff and Class members without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), Marriott has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class members.

174. Marriott's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

175. Under the common law doctrine of unjust enrichment, it is inequitable for Marriott to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and Class members in an unfair and unconscionable manner. Marriott's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

176. The benefit conferred upon, received, and enjoyed by Marriott was not conferred officiously or gratuitously, and it would be inequitable and unjust for Marriott to retain the benefit.

177. Marriott is therefore liable to Plaintiff and Class members for restitution in the amount of the benefit conferred on Marriott as a result of its wrongful conduct, including specifically the value to Marriott of the Personal Information that was stolen in the Starwood Breach and the profits Marriott is receiving from the use and sale of that information.

COUNT IX

Declaratory Judgment

(Against Marriott International and Starwood)

(On Behalf of Plaintiff and All Class Members)

178. Plaintiff, individually and on behalf of all Class members, restates and realleges the foregoing allegations as if fully set forth herein.

179. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

180. An actual controversy has arisen in the wake of the Starwood Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Marriott is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Personal Information. Plaintiff and Class members allege that Marriott's data security measures remain inadequate. Marriott denies these allegations. Furthermore, Plaintiff and Class members continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

181. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Marriott continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

(b) Marriott continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

182. The Court also should issue corresponding prospective injunctive relief requiring Marriott to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

183. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Marriott.

184. The risk of another such breach is real, immediate, and substantial. If another breach at Marriott occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

185. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Marriott if an injunction is issued. Among other things, if another massive data breach occurs at Marriott, Plaintiff and Class members will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Marriott of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Marriott has a pre-existing legal obligation to employ such measures.

186. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Marriott, thus eliminating the additional injuries that would result to Plaintiff and Class members and the millions of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and all others similarly situated, respectfully requests that this Court enter judgment against Defendants and in favor of Plaintiff and the Classes, and award the following relief:

a) That the Court determine that this action may be maintained as a class action under Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure and direct that reasonable notice of this action, as provided by Rule 23(c)(2) of the Federal Rules of Civil Procedure, be given to Class members;

b) Monetary damages in excess of $5,000,000;

c) Injunctive relief, including but not limited to the provision of credit monitoring services for a period of at least 25 years, the provision of bank monitoring services for a period of at least 25 years, the provision of credit restoration services for a period of at least 25 years, and the provision of identity theft insurance for a period of at least 25 years;

d) That the Court award Plaintiff and the Classes attorneys' fees and costs, including expert and consultant fees, as well as pre-judgment and post-judgment interest as permitted by law; and

e) That the Court award Plaintiff and the Classes such other and further relief as may be deemed necessary and appropriate.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: December 19, 2018

Respectfully submitted,

LAW OFFICES OF SUSAN R. PODOLSKY

By: /s/ Susan R. Podolsky

Susan R. Podolsky (Bar No. 22916)
1800 Diagonal Road
Suite 600
Alexandria, VA 22314
spodolsky@podolskylaw.com
Tel: (571) 366-1702
Fax: (703) 647-6009

BLEICHMAR FONTI & AULD LLP

Lesley E. Weaver
555 12th Street, Suite 1600
Oakland, CA 94607
lweaver@bfalaw.com
Tel: (415) 445-4003
Fax : (415) 445-4004

Counsel for Plaintiff